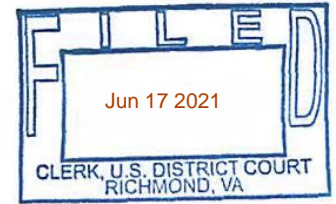


**IN THE UNITED STATES DISTRICT COURT FOR THE  
EASTERN DISTRICT OF VIRGINIA  
Richmond Division**



IN THE MATTER OF THE SEARCH OF:

- (a) THE PERSON OF GEOFFREY WILLIAM SILLS
- (b) 8276 SHANE EDMONDS LANE, MECHANICSVILLE, VA. 23111
- (c) MOBILE DEVICES BELONGING TO GEOFFREY WILLIAM SILLS

**FILED UNDER SEAL**

Case No. 3:21-sw-86

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

**I. Introduction**

Your Affiant, Benjamin Fulp, being first duly sworn, does hereby depose and state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2018. During that time, I have investigated kidnappings, bank robberies, fugitive matters, Hobbs Act violations, Felon in Possession violations, and threat-to-life violations as a part of the FBI Washington Field Office Violent Crimes Task Force. I have prepared and assisted in the preparation of court orders and search warrant applications. Additionally, during the course of these and other investigations, I have conducted or participated in physical and electronic surveillance, assisted in the execution of search and arrest warrants, debriefed informants, interviewed witnesses and suspects, and reviewed other pertinent records. I have received training through the FBI's Cellular Analysis and Survey Team (CAST) program to

evaluate cellular records for evidentiary value. Through my training, education, and experience, I have become familiar with the efforts of persons involved in criminal activity to avoid detection by law enforcement. I am assisting in the investigation and prosecution of events which occurred at the United States Capitol on January 6, 2020. Currently, I am tasked with investigating criminal activity in and around the U.S. Capitol grounds on January 6, 2021. As a Special Agent of the FBI, I am authorized by law or by a government agency to engage in or supervise the prevention, detection, investigation, or prosecution of a violation of federal criminal laws.

## **II. Reason for Affidavit**

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. This affidavit is made in support of an application for a search warrant for the following location:

- a. **The person of GEOFFREY WILLIAM SILLS (or hereinafter “SILLS’ PERSON”)**, as further described in Attachment A, and any electronic devices located on the person of **SILLS**. The items to be seized are described in the following paragraphs and in Attachment B.
- b. **SILLS’s residence located at 8276 Shane Edmonds Lane, Mechanicsville, VA. 23111 (or hereinafter “the SUBJECT RESIDENCE”)**, as further described in Attachment A, as a two story white single family home, with dark shutters, a light green front door, and a light green door on the side of the driveway.

- c. **Mobile device belonging to SILLS, (or hereinafter “the SUBJECT DEVICE”)** which is further described and depicted in Attachment A. The items to be searched and seized are described in the following paragraphs and in Attachment B.

4. Based on the information set forth herein, your Affiant has probable cause to believe (a) that **SILLS** engaged in violations of Title 18, United States Code, § 111(a)(1) and (b), Title 18 United States Code, § 231(a)(3), Title 18 United States Code, § 1512(c)(2) and 2, Title 18 United States Code, § 1752(a)(4), and Title 40 United States Code, § 5104(e)(2)(F); and (b) that other identified and unidentified persons, including others who may have been aided and abetted by, or conspiring with, **SILLS**, as well as others observed by **SILLS**, engaged in violations of 18 U.S.C. §§ 1512(c)(2) (obstruction of Congress); 111 (assaulting a federal agent); 231 (civil disorders), 371 (conspiracy); 372 (conspiracy to impede or injure officer); 930 (possession of firearms and dangerous weapons in federal facilities); 641 (theft of government property); 1361 (destruction of government property); 2101 (interstate travel to participate in riot); 1752(a)(1) and (2) (unlawful entry on restricted buildings or grounds); and Title 40 U.S.C. Section 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds), and that evidence and instrumentalities related to these violations (collectively, the “Target Offenses”), as further described in Attachment B, may be found on **SILLS’s PERSON**, at the **SUBJECT RESIDENCE**, and on the **SUBJECT DEVICE(S)**.

5. This affidavit is based upon information that I have gained from my investigation, my training and experience, as well as information gained from conversations with other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation.

I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence and instrumentalities (more precisely described in Attachment B) of the Target Offenses are located on **SILLS's PERSON**, at the **SUBJECT RESIDENCE**, and on the **SUBJECT DEVICES** (as further described in Attachment A).

6. This investigation involves evidence and instrumentalities of offenses within the jurisdiction and proper venue of the United States District Court for the Eastern District of Virginia, as more fully articulated herein.

### **III. Pertinent Federal Criminal Statutes and Definitions**

7. This investigation concerns alleged violations of:
- a. 18 U.S.C. § 111(a)(1) and (b), which makes it a crime to forcibly assault, resist, oppose, impede, intimidate, or interfere with any person designated in 18 U.S.C. § 1114 as an officer or employee of the United States while engaged in or on account of the performance of official duties. Persons designated within section 1114 include any person assisting an officer or employee of the United States in the performance of their official duties. Subdivision (b) provides for enhanced penalties when bodily injury is inflicted or a dangerous weapon is used.
  - b. 18 U.S.C. § 231(a)(3), which makes it unlawful to commit or attempt to commit any act to obstruct, impede, or interfere with any fireman or law enforcement officer lawfully engaged in the lawful performance of his official duties incident to and during the commission of a civil disorder which in any way or degree obstructs, delays, or adversely affects commerce or the movement of any article or commodity in commerce or the conduct or performance of any federally protected function. For purposes of Section 231 of Title 18, a federally protected function means any function, operation, or action carried out, under the laws of the United States, by any department, agency, or instrumentality of

the United States or by an officer or employee thereof. This includes the Joint Session of Congress where the Senate and House count Electoral College votes.

c. 18 U.S.C. §§ 1512(c)(2) and 2, which makes it a crime to obstruct, influence, or impede any official proceeding, or attempt to do so. Under 18 U.S.C. § 1515, congressional proceedings are official proceedings.

d. 18 U.S.C. § 1752(a)(1), (2), and (4), which makes it a crime to (1) knowingly enter or remain in any restricted building or grounds without lawful authority to do; and (2) knowingly, and with intent to impede or disrupt the orderly conduct of government business or official functions, engage in disorderly or disruptive conduct in, or within such proximity to, any restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of government business or official functions; (4) knowingly engage in any act of physical violence against any person or property in any restricted building or grounds, or attempt or conspire to do so. For purposes of Section 1752 of Title 18, a “restricted building” includes a posted, cordoned off, or otherwise restricted area of a building or grounds where the President or other person protected by the Secret Service, including the Vice President, is or will be temporarily visiting; or any building or grounds so restricted in conjunction with an event designated as a special event of national significance.

e. 40 U.S.C. § 5104(e)(2)(D), (F), and (G), which makes it a crime to willfully and knowingly (D) utter loud, threatening, or abusive language, or engage in disorderly or disruptive conduct, at any place in the grounds or in any of the Capitol Buildings with the intent to impede, disrupt, or disturb the orderly conduct of a session of Congress or either House of Congress, or the orderly

conduct in that building of a hearing before, or any deliberations of, a committee of Congress or either House of Congress; (F) engage in an act of physical violence in the grounds or any of the Capitol Buildings; and (G) parade, demonstrate, or picket in any of the Capitol Buildings.

f. 18 U.S.C. § 371, which makes it a crime for two or more persons to conspire either to commit any offense against the United States, or to defraud the United States, or any agency thereof in any manner or for any purpose, when one or more of such persons do any act to effect the object of the conspiracy.

g. 18 U.S.C. § 372, which makes it a crime for two or more persons in any State, Territory, Possession, or District to conspire to prevent, by force, intimidation, or threat, any person from accepting or holding any office, trust, or place of confidence under the United States, or from discharging any duties thereof, or to induce by like means any officer of the United States to leave the place, where his duties as an officer are required to be performed, or to injure him in his person or property on account of his lawful discharge of the duties of his office, or while engaged in the lawful discharge thereof, or to injure his property so as to molest, interrupt, hinder, or impede him in the discharge of his official duties.

h. 18 U.S.C. § 930, which makes it a crime to knowingly possess or cause to be present a firearm or other dangerous weapon in a Federal facility (other than a Federal court facility) or attempt to do so and knowingly possess or cause to be present such firearm or dangerous weapon in a Federal facility with intent that a firearm or other dangerous weapon be used in the commission of a crime or attempt to do so.

- i. 18 U.S.C. § 641, which makes it a crime to embezzle, steal, purloin, or knowingly convert to his use or the use of another, or without authority, sell, convey or dispose of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof and to receive, conceal, or retain the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted.
- j. 18 U.S.C. § 1361, which makes it a crime to willfully injure or commit any depredation against any property of the United States, or of any department or agency thereof, or any property which has been or is being manufactured or constructed for the United States, or any department or agency thereof, or attempt to commit any of the foregoing offenses.
- k. 18 U.S.C. § 2101, which makes it a crime to travel in interstate or foreign commerce or use any facility of interstate or foreign commerce, including, but not limited to, the mail, telegraph, telephone, radio, or television, with intent—  
(1) to incite a riot; or (2) to organize, promote, encourage, participate in, or carry on a riot; or (3) to commit any act of violence in furtherance of a riot; or (4) to aid or abet any person in inciting or participating in or carrying on a riot or committing any act of violence in furtherance of a riot; and to either during the course of any such travel or use or thereafter perform or attempt to perform any other overt act for those purposes.
- l. 18 U.S.C. § 2111, which makes it a crime to, within the special maritime and territorial jurisdiction of the United States, by force and violence, or by

intimidation, take or attempt to take from the person or presence of another anything of value.

#### **IV. Background of the Investigation and Probable Cause**

8. U.S. Capitol Police (USCP), the FBI, and assisting law enforcement agencies are investigating a riot and related offenses that occurred at the United States Capitol Building, located at 1 First Street, NW, Washington, D.C., 20510 at latitude 38.88997 and longitude -77.00906 on January 6, 2021.

9. At the U.S. Capitol, the building itself has 540 rooms covering 175,170 square feet of ground, roughly four acres. The building is 751 feet long (roughly 228 meters) from north to south and 350 feet wide (106 meters) at its widest point. The U.S. Capitol Visitor Center is 580,000 square feet and is located underground on the east side of the Capitol. On the west side of the Capitol building is the West Front, which includes the inaugural stage scaffolding, a variety of open concrete spaces, a fountain surrounded by a walkway, two broad staircases, and multiple terraces at each floor. On the East Front are three staircases, porticos on both the House and Senate side, and two large skylights into the Visitor's Center surrounded by a concrete parkway. All of this area was barricaded and off limits to the public on January 6, 2021.

10. The U.S. Capitol is secured 24 hours a day by USCP. Restrictions around the U.S. Capitol include permanent and temporary security barriers and posts manned by USCP. Only authorized people with appropriate identification are allowed access inside the U.S. Capitol.

11. On January 6, 2021, the exterior plaza of the U.S. Capitol was closed to members of the public.

12. On January 6, 2021, a joint session of the United States Congress convened at the U.S. Capitol. During the joint session, elected members of the United States House of



Representatives and the United States Senate were meeting in separate chambers of the U.S. Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election, which took place on November 3, 2020 (“Certification”). The joint session began at approximately 1:00 p.m. Eastern Standard Time (EST). Shortly thereafter, by approximately 1:30 p.m. EST, the House and Senate adjourned to separate chambers to resolve a particular objection. Vice President Mike Pence was present and presiding, first in the joint session, and then in the Senate chamber.

13. As the proceedings continued in both the House and the Senate, and with Vice President Mike Pence present and presiding over the Senate, a large crowd gathered outside the U.S. Capitol. As noted above, temporary and permanent barricades were in place around the exterior of the U.S. Capitol building, and USCP were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside.

14. At around 1:00 p.m. EST, known and unknown individuals broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past USCP and supporting law enforcement officers there to protect the U.S. Capitol.

15. At around 1:30 p.m. EST, USCP ordered Congressional staff to evacuate the House Cannon Office Building and the Library of Congress James Madison Memorial Building in part because of a suspicious package found nearby. Pipe bombs were later found near both the Democratic National Committee and Republican National Committee headquarters.

16. Media reporting showed a group of individuals outside of the Capitol chanting, “Hang Mike Pence.” I know from this investigation that some individuals believed that Vice President Pence possessed the ability to prevent the certification of the presidential election and that his failure to do so made him a traitor.

17. At approximately 2:00 p.m. EST, some people in the crowd forced their way through, up, and over the barricades and law enforcement. The crowd advanced to the exterior façade of the building. The crowd was not lawfully authorized to enter or remain in the building and, prior to entering the building, no members of the crowd submitted to security screenings or weapons checks by U.S. Capitol Police Officers or other authorized security officials. At such time, the certification proceedings were still underway and the exterior doors and windows of the U.S. Capitol were locked or otherwise secured. Members of law enforcement attempted to maintain order and keep the crowd from entering the Capitol.

18. Shortly after 2:00 p.m. EST, individuals in the crowd forced entry into the U.S. Capitol, including by breaking windows and by assaulting members of law enforcement, as others in the crowd encouraged and assisted those acts. Publicly available video footage shows an unknown individual saying to a crowd outside the Capitol building, “We’re gonna fucking take this,” which your Affiant believes was a reference to “taking” the U.S. Capitol.



19. Shortly thereafter, at approximately 2:20 p.m. EST, members of the United States House of Representatives and United States Senate, including the President of the Senate, Vice President Mike Pence, were instructed to—and did—evacuate the chambers. That is, at or about this time, USCP ordered all nearby staff, Senators, and reporters into the Senate chamber and locked it down. USCP ordered a similar lockdown in the House chamber. As the subjects attempted to break into the House chamber, by breaking the windows on the chamber door, law enforcement were forced to draw their weapons to protect the victims sheltering inside.

20. At approximately 2:30 p.m. EST, known and unknown subjects broke windows and pushed past USCP and supporting law enforcement officers forcing their way into the U.S. Capitol on both the west side and the east side of the building. Once inside, the subjects broke windows and doors, destroyed property, stole property, and assaulted federal police officers. Many of the federal police officers were injured and several were admitted to the hospital. The subjects also confronted and terrorized members of Congress, Congressional staff, and the media. The subjects carried weapons including tire irons, sledgehammers, bear spray, and tasers. They also took police equipment from overrun police including shields and police batons. At least one of the subjects carried a handgun with an extended magazine. These actions by the unknown individuals resulted in the disruption and ultimate delay of the vote Certification.

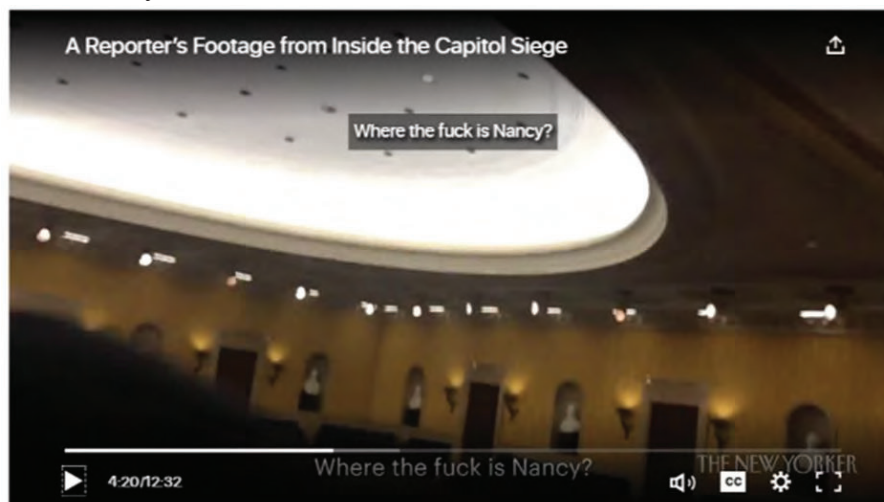
21. Also at approximately 2:30 p.m. EST, USCP ordered the evacuation of lawmakers, Vice President Mike Pence, and president pro tempore of the Senate, Charles Grassley, for their safety.

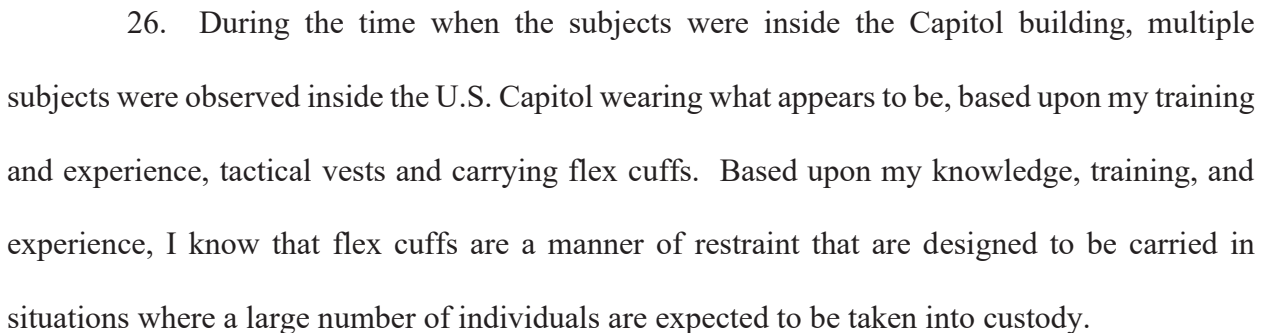
22. At around 2:45 p.m. EST, subjects broke into the office of House Speaker Nancy Pelosi.

23. At around 2:47 p.m. EST, subjects broke into the United States Senate Chamber. Publicly available video shows an individual asking, “Where are they?” as they opened up the door to the Senate Chamber. Based upon the context, law enforcement believes that the word “they” is in reference to members of Congress.



24. After subjects forced entry into the Senate Chamber, publicly available video shows that an individual asked, “Where the fuck is Nancy?” Based upon other comments and the context, law enforcement believes that the “Nancy” being referenced was the Speaker of the House of Representatives, Nancy Pelosi.









27. At around 2:45 p.m. EST, one subject was shot and killed while attempting to break into the House chamber through the broken windows.

28. At around 2:48 p.m. EST, DC Mayor Muriel Bowser announced a citywide curfew beginning at 6:00 p.m. EST.

29. At about 3:25 p.m. EST, law enforcement officers cleared the Senate floor.

30. Between 3:25 and around 6:30 p.m. EST, law enforcement was able to clear the U.S. Capitol of all of the subjects.

31. Based on these events, all proceedings of the United States Congress, including the joint session, were effectively suspended until shortly after 8:00 p.m. EST the same day. In light of the dangerous circumstances caused by the unlawful entry to the U.S. Capitol, including the

danger posed by individuals who had entered the U.S. Capitol without any security screening or weapons check, Congressional proceedings could not resume until after every unauthorized occupant had left the U.S. Capitol, and the building had been confirmed secured. The proceedings resumed at approximately 8:00 pm after the building had been secured. Vice President Pence remained in the United States Capitol from the time he was evacuated from the Senate Chamber until the session resumed.

32. Beginning around 8:00 p.m. EST, the Senate resumed work on the Certification.

33. Beginning around 9:00 p.m. EST, the House resumed work on the Certification.

34. Both chambers of Congress met and worked on the Certification within the Capitol building until approximately 3:00 a.m. EST on January 7, 2021.

35. During national news coverage of the aforementioned events, video footage which appeared to be captured on mobile devices of persons present on the scene depicted evidence of violations of local and federal law, including scores of individuals inside the U.S. Capitol building without authority to be there.

36. Based on my training and experience, I know that it is common for individuals to carry and use their cell phones during large gatherings, such as the gathering that occurred in the area of the U.S. Capitol on January 6, 2021. Such phones are typically carried at such gatherings to allow individuals to capture photographs and video footage of the gatherings, to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings.

37. Many subjects seen on news footage in the area of the U.S. Capitol are using a cell phone in some capacity. It appears some subjects were recording the events occurring in and

around the U.S. Capitol and others appear to be taking photos, to include photos and video of themselves after breaking into the U.S. Capitol itself, including photos of themselves damaging and stealing property. As reported in the news media, others inside and immediately outside the U.S. Capitol live-streamed their activities, including those described above as well as statements about these activities.

38. Photos below, available on various publicly available news, social media, and other media show some of the subjects within the U.S. Capitol during the riot. In several of these photos, the individuals who broke into the U.S. Capitol can be seen holding and using cell phones, including to take pictures and/or videos:



1

---

<sup>1</sup> <https://losangeles.cbslocal.com/2021/01/06/congresswoman-capitol-building-takeover-an-attempted-coup/>





### **Facts Specific to this Application**

39. Based on an initial review of publicly available video footage, USCP surveillance footage, and body worn camera (“BWC”) footage of officers that responded to the Capitol on January 6, 2021, a white male with brown hair, who was wearing a black “Make America Great

---

<sup>2</sup> <https://www.businessinsider.com/republicans-objecting-to-electoral-votes-in-congress-live-updates-2021-1>

<sup>3</sup> <https://www.thv11.com/article/news/arkansas-man-storms-capitol-pelosi/91-41abde60-a390-4a9e-b5f3-d80b0b96141e>

Again” (MAGA) hat, a distinctive striped shirt, black binoculars, a black gas mask, black and white sneakers, a white gauge ear piercing, and a black and grey backpack, who has been identified as SILLS, as described below, can be seen repeatedly assaulting multiple law enforcement officers guarding the Capitol. SILLS is pictured in the two still shots below with a red box added around SILLS in the second one.

*Screenshot from Video Posted on YouTube (hereinafter “YouTube Video 1”)*



*Screenshot from BWC Footage*



*Identification of SILLS*

40. On approximately January 25, 2021, SILLS, who was unidentified at the time, was included in a “Seeking Information” list and given the moniker “153-AFO.” The FBI posted that list to its website and to social media to garner public assistance to identify the individual.



# SEEKING INFORMATION

## ASSAULT ON FEDERAL OFFICERS AND VIOLENCE AT THE UNITED STATES CAPITOL

WASHINGTON, D.C.  
JANUARY 6, 2021



Photograph #145-AFO      Photograph #146-AFO      Photograph #147-AFO      Photograph #148-AFO      Photograph #149-AFO



Photograph #150-AFO      Photograph #151-AFO      Photograph #152-AFO      Photograph #153-AFO      Photograph #154-AFO

### DETAILS

The Federal Bureau of Investigation's (FBI) Washington Field Office is seeking the public's assistance in identifying individuals who made unlawful entry into the United States Capitol Building and assaulted federal law enforcement personnel on January 6, 2021, in Washington, D.C.

Anyone with information regarding these individuals, or anyone who witnessed any unlawful violent actions at the Capitol or near the area, is asked to contact the FBI's Toll-Free Tipline at 1-800-CALL-FBI (1-800-225-5324) to verbally report tips. You may also submit any information that could be relevant online at [tips.fbi.gov](https://tips.fbi.gov). You may also contact your local FBI office or the nearest American Embassy or Consulate.

When providing a tip on one of these individuals, please reference "AFO" and the photo number.

**Field Office:** Washington D.C.

41. On approximately February 16, 2021, the FBI identified two photographs, via the Sedition Hunters Twitter account, of 153-AFO without his mask and holding his black MAGA hat in his hand; the FBI updated the photograph for "153-AFO" accordingly.

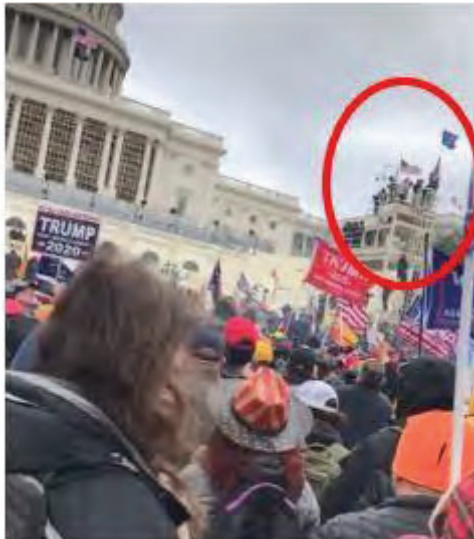


*Photographs from Twitter Account @SeditionHunters*

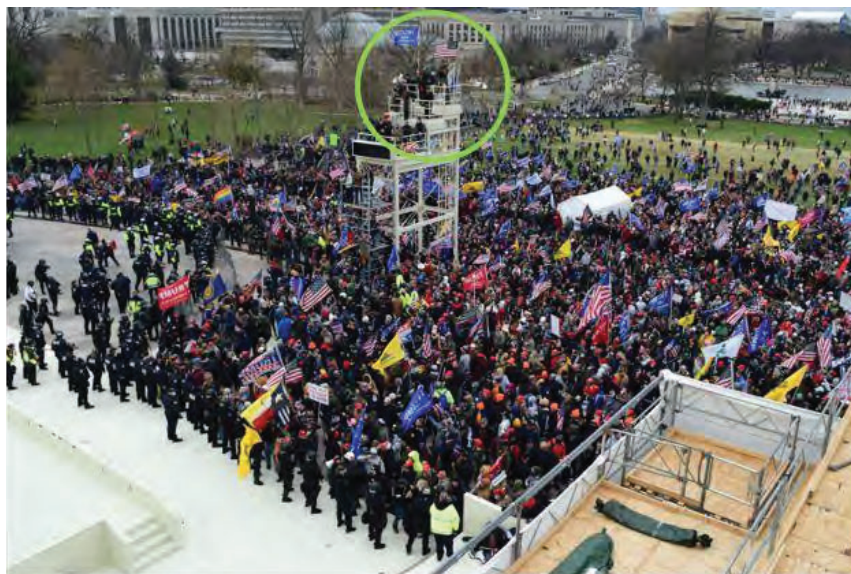


42. Your affiant has reviewed the video from which these two photographs were pulled. The video, which appears to have been posted to TikTok, is filmed outside of the Capitol likely sometime after 1 p.m. (hereinafter “TikTok Video 1”). Your affiant has compared the scene visible in TikTok Video 1 to videos and photographs filmed by USCP officers on January 6, 2021. Your affiant has been able to corroborate the video by identifying what appear to be the some of the same events filmed at a different angle. For instance, in TikTok Video 1, rioters can be seen on top of the tower with a blue flag and a U.S. flag, as shown in red circle in the still below. The same events can be seen in a photograph taken by USCP around 1 p.m., as shown in the green circle below. During the investigation, law enforcement received information from five tipsters regarding the identification of SILLS.

*Still from TikTok Video 1*



*Photo by USCP*



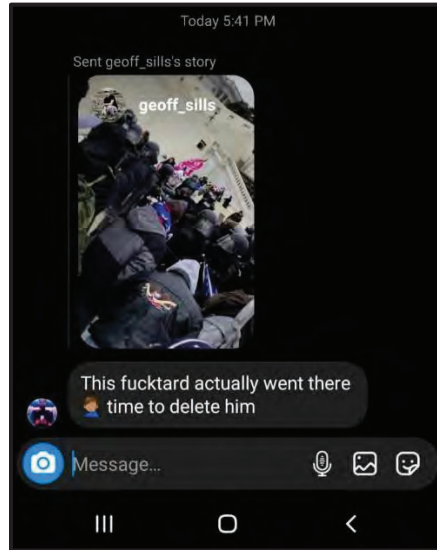
43. On or around January 8, 2021, a known individual (hereinafter “Witness 1”) submitted an online tip through the FBI Office of Public Affairs (OPA) online portal and indicated

that on January 6, 2021, “Geoffrey William Sills” posted a video on SILLS’s Instagram account, “geoff\_sills,” depicting what appears to be SILLS entering the Capitol during the breach. Witness 1 described how he/she knew SILLS as an acquaintance and explained he/she had attended college with SILLS from 2009 to 2013. Along with this information, Witness 1 provided the following images. (The Instagram account “geoff\_sills” appears to have been deleted or the username has changed as it is no longer online.)

*Photograph of Geoffrey Sills Provided by Witness 1*



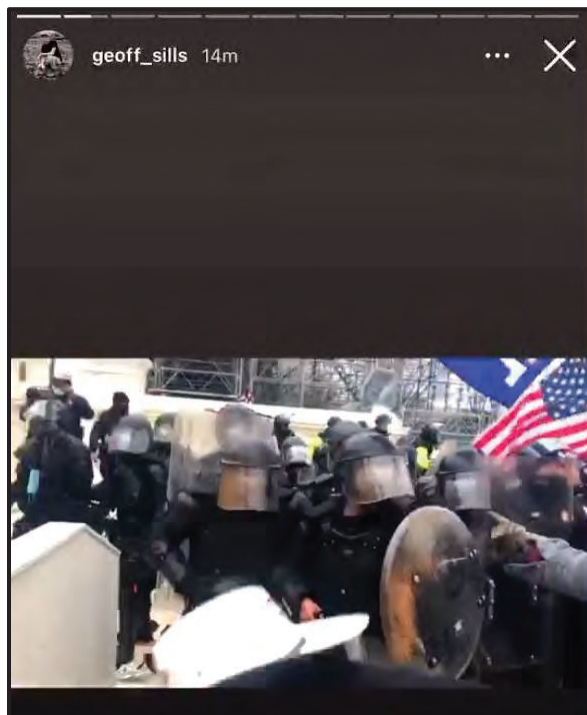


*Photograph of Instagram Account Provided by Witness 1*

44. On or around January 11, 2021, a known individual (hereinafter “Witness 2”) submitted an online tip through the OPA online portal and indicated that Instagram account “@geoff\_sills” posted a video on January 6, 2021 around 7:00 p.m. (Eastern Standard Time) of rioters smashing windows to get inside the Capitol building and hitting armed police officers to get inside. Along with this information, Witness 2 provided a copy of the Instagram video posted by Instagram account “@geoff\_sills” (hereinafter “@geoff\_sills Instagram video”). Your affiant reviewed the video, which revealed it was a compilation of various videos taken at the U.S. Capitol on January 6, 2021. BWC footage from various MPD officers and USCP surveillance footage captures some of these same events and also shows SILLS with a phone in his hand as if he was recording.

45. For example, the below screenshot from the @geoff\_sills Instagram video corresponds with the same events around 2:31 p.m. captured on BWC from the opposite perspective, as shown in the screenshot below, with a yellow circle added around SILLS.

*Screenshot from @geoff\_sills Instagram video*



*Screenshot from BWC of MPD Officer 2*



46. Similarly, the below screenshot from the @geoff\_sills Instagram video corresponds with the same events captured on USCP surveillance footage around 2:41 p.m. from the opposite perspective, as shown in the screenshot below with a red circle added around SILLS.

*Screenshot from @geoff\_sills Instagram video*

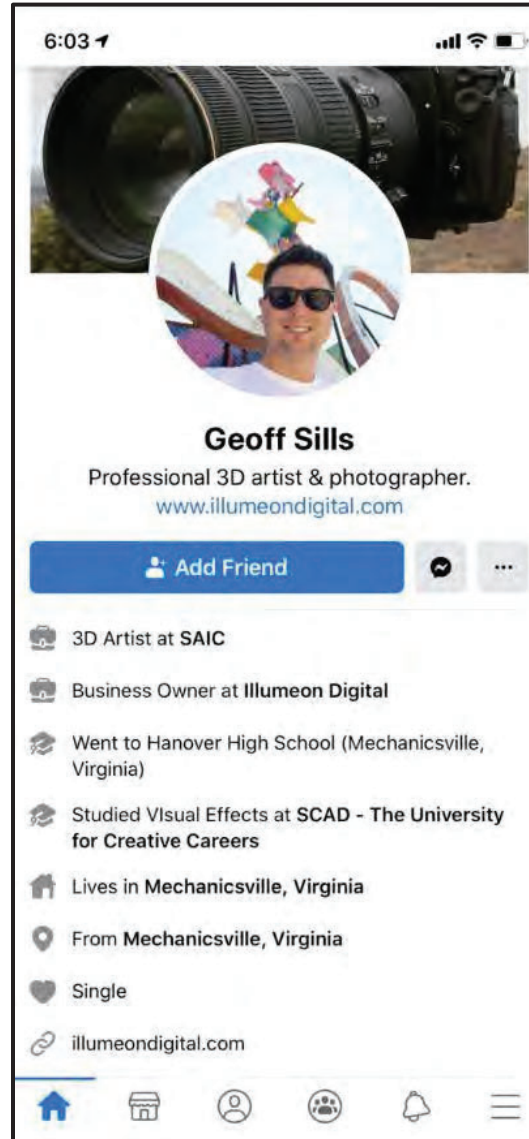


*Screenshot from USCP Surveillance Footage*



47. On January 12, 2021, a known individual (hereinafter “Witness 3”) submitted an online tip through the OPA online portal and indicated that “Geoff Sills,” who is originally from Mechanicsville, Virginia, and currently resides in Huntsville, Alabama, posted multiple Instagram stories of his participation in storming the Capitol. Along with this information, Witness 3 provided a copy of the same aforementioned video provided by Witness 2 and provided the following image. Witness 1 viewed the @geoff\_sills Instagram video provided by Witness 2 and Witness 3. Witness 1 confirmed that this was the same video Witness 1 saw posted on January 6, 2021 on the Instagram account Witness 1 knows to belong to SILLS.

*Photograph Provided by Witness 3*



48. On March 23, 2021, subsequent to the distribution of the 153-AFO seeking information flyer, two known individuals (hereinafter "Witness 4" and "Witness 5") called the FBI National Threat Operations Center (NTOC) and indicated that 153-AFO bore a resemblance to "Geoff Sills." Witness 4 and Witness 5, who are both current employees of the company "MicroD," described how they knew SILLS and indicated that SILLS was a former MicroD

employee who was hired in 2018 and terminated on January 13, 2020. Witnesses 4 and 5 were also able to provide the date of birth for SILLS.

49. On March 29, 2021, your affiant interviewed Witnesses 4 and 5 who provided additional information regarding SILLS. During the interview, Witness 5 indicated that on or about March 22, 2021, an individual on Twitter tagged @MicroDinc in a Twitter post identifying the backpack worn by 153-AFO as depicting the MicroD company logo on it. That backpack was given to employees as a gift approximately four years ago and was only issued one time. Witnesses 4 and 5 reviewed the images on Twitter and noticed 153-AFO had gauged earrings and confirmed that the backpack was the same as the one given out by the company. They could only recall one employee from that timeframe who had gauged earrings, SILLS. Furthermore, after reviewing the photograph released by the FBI depicting 153-AFO, they noticed that the striped shirt 153-AFO wore appeared to be the same one that SILLS wore to a company social event held several years ago and that they retained pictures of. Witness 4 stated that he/she was “90-99%” and “the best possible score I can give” regarding Witness 4’s certainty that 153-AFO was SILLS. Witness 4 also provided the following photographs of SILLS wearing the striped shirt that appeared to be the same one worn by 153-AFO. Witnesses 4 and 5 have not seen SILLS in over a year.



*Photographs Provided by Witness 4*



50. In addition to the photographs provided by Witness 4 of SILLIS wearing what appears to be the same striped shirt, your affiant reviewed and compared a screenshot of 153-AFO with SILLIS's North Carolina driver's license photo that was issued in 2019, in which SILLIS has what appears to be the same white gauge ear piercings as 153-AFO.

51. Finally, based on a review of financial records obtained by subpoena, SILLIS appears to have made a purchase at a Metro station in Franconia-Springfield on January 6, 2021. That Metro stop has Metro trains that go into Washington, D.C., indicating that SILLIS was in the Washington, D.C. area on that day. The same financial account records also show multiple purchases at stores in November 2020 (including "Infidel Body Armor," "Freedom Fighters Tactic," and "Cheaper than Dirt"), which based on their websites sell body armor, weapons, gas masks, and/or other combat equipment. The records also show multiple purchases at Bass Pro

Shop in November – a store that sells collapsible batons and LED flashlights similar to the ones used by SILLS on January 6, 2020, in addition to a variety of outdoor sporting equipment.

52. According to records obtained through a search warrant served on Verizon Wireless, the cellphone associated with number (XXX) XXX-5712 (hereinafter the “SUBJECT PHONE NUMBER”), was identified as having utilized a cell site consistent with providing service to a geographic area that includes the interior of the United States Capitol building on and around the date of January 6, 2021. Witness 4 provided the SUBJECT PHONE NUMBER as the account belonging to SILLS. A review of records provided by Verizon Wireless in response to a subpoena indicate that the mother of SILLS is currently the financially liable party for the SUBJECT PHONE NUMBER and has been a Verizon customer since March 2008. The number is linked to an iPhone 7 Plus with IMEI 359475084846204. Subscriber records also show that the phone was active repeatedly from January 5 to January 7, 2021, with calls made or received each day. Your affiant has also reviewed financial records for an account belonging to SILLS. The records further list the SUBJECT PHONE NUMBER as belonging to SILLS.

53. Law enforcement also received six tips indicating that 153-AFO looked like various individuals that are not SILLS. Law enforcement has followed up on each of the tips to the extent possible given the information provided. Thus far, your affiant is not aware of any corroboration for these tips and is not aware of any evidence linking those individuals to the Capitol on January 6, 2021.

54. Your affiant is not aware of any other information provided to the FBI about SILLS or 153-AFO at this time. However, the FBI is receiving tips from throughout the country on a daily basis about individuals who may have participated in the events at the Capitol on January 6, 2021.



*Actions by SILLS on January 6, 2021*

55. As captured on USCP surveillance, BWC footage, and various videos posted to social media and YouTube, on January 6, 2021, law enforcement to include USCP and MPD were along a temporary fence line in the Lower West Terrace area of the Capitol. Law enforcement stood behind the metal fencing shoulder to shoulder. As time moved on, the crowd started to push and tear down the fencing separating the crowd and law enforcement. Law enforcement attempted to push back and reestablish the fence line. During this time objects were thrown at officers, physical assaults occurred, and chemical irritants were used by the crowd. At approximately 2:28 p.m., rioters were breaching the line of law enforcement and successfully advancing towards the first landing of the Lower West Terrace. During the breach, multiple officers were assaulted. SILLS is visible on BWC footage near the front lines of the rioters surrounding the officers as they were forced to retreat, and SILLS can be seen repeatedly throwing items at the officers.

56. Specifically, at approximately 2:28 p.m., SILLS is captured on the BWC of a known MPD Officer (hereinafter MPD Officer 1) during the aforementioned breach that occurred on and near the Lower West Terrace. SILLS appears to be taking a video, using his phone, of officers being assaulted by other rioters.

*Screenshot from BWC of MPD Officer 1*



57. From approximately 2:29 p.m. to 2:31 p.m., SILLS was captured on the BWC of additional known MPD Officers (hereinafter MPD Officer 2 and MPD Officer 3) and appears to have advanced to the first landing of the Lower West Terrace.

*Screenshot from BWC of MPD Officer 2*



*Screenshot from BWC of MPD Officer 3*



58. At approximately 2:31 p.m., SILLS was captured on the BWC of MPD Officer 2 on the first landing of the Lower West Terrace appearing to take a video of multiple USCP officers being assaulted by other rioters, including a rioter who strikes a USCP officer to the ground, as seen in the screenshot below with a yellow circle around SILLS. As described above, the screenshot below also corresponds exactly to the video SILLS posted on his Instagram account and indicates that SILLS was in fact taking the video himself using his phone.

*Screenshot from BWC of MPD Officer 2*



59. As captured on BWC footage, law enforcement officers continued to retreat backwards and fell back into a stairwell. In addition to being captured on BWC footage, these same events, and SILLS, were also variously captured on videos posted online. For example, SILLS is similarly visible at the forefront of the rioters in YouTube Video 1 and in a video published by the New York Times (hereinafter “New York Times Video”), as shown in the still shots below with a red circle around SILLS.

*Screenshot from YouTube Video 1*



*Screenshot Derived New York Times Video*



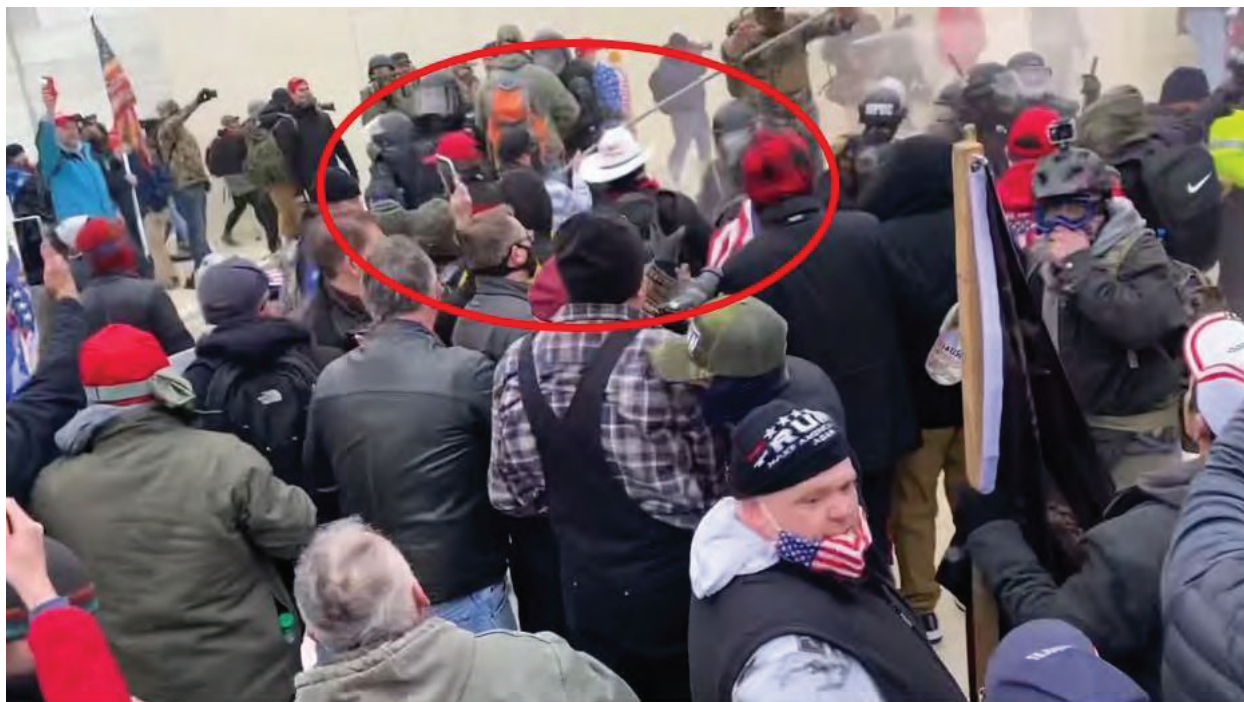
60. SILLS is also captured throwing multiple objects at law enforcement as they retreated, as captured in another video uploaded to YouTube (hereinafter “YouTube Video 2”). YouTube Video 2 was filmed by another rioter (who has since been arrested) and was obtained through a search warrant of his related account.

61. Specifically, around 5 minutes and 23 seconds into YouTube Video 2, SILLS can be seen throwing what appears to be a long pole at law enforcement, as shown in the still below



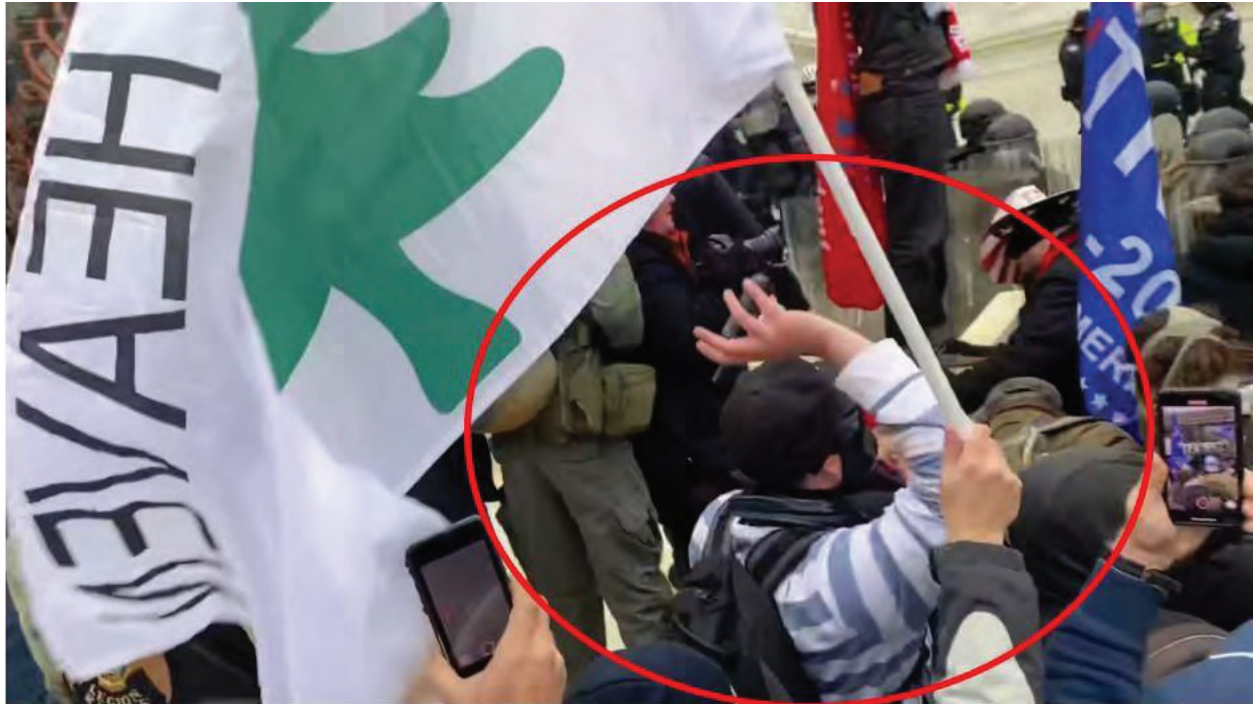
with a red circle around SILLS. Around this time, other rioters are also throwing objects at the officers, as captured both on YouTube Video 2 and BWC footage.

*Screenshot from YouTube Video 2*



62. Then around 7 minutes and 42 seconds into YouTube Video 2, SILLS can be seen picking up an unknown object and throwing it at law enforcement, as shown in the still below with a red circle around SILLS. SILLS can then be seen throwing a small black pole at law enforcement. Based on a comparison with BWC from Officer 1, which captures some of the same events from a different perspective, this likely occurred around 2:32 p.m.

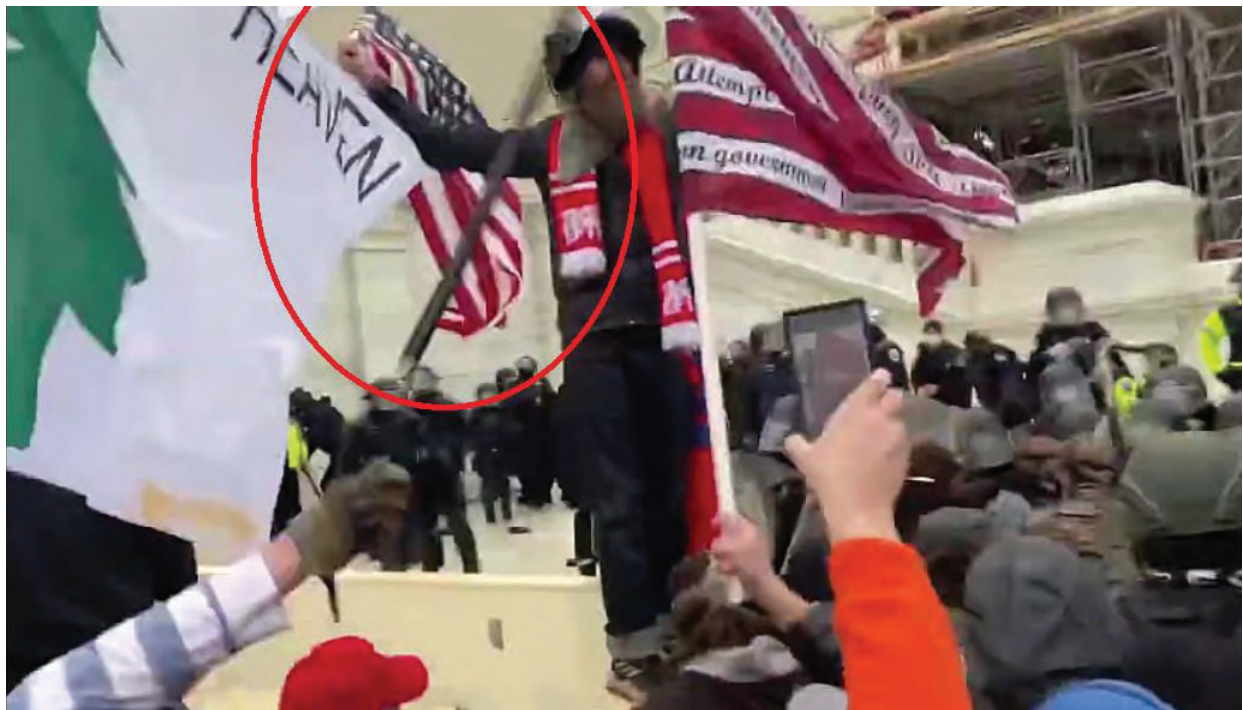
*Screenshot from YouTube Video 2*



63. Then around 8 minutes into YouTube Video 2, SILLS can be seen throwing another pole or stick at law enforcement, as shown in the still below with a red circle around SILLS and the item.



*Screenshots from YouTube Video 2*



64. As captured in YouTube Video 2 and BWC footage, officers continued to retreat into the door behind them, which was the door built into the inaugural platform. Based on a review

of a map of U.S. Capitol grounds, this door appears to be an access point to the stairwell that leads to next level of the Lower West Terrace where the tunnel that led to the Lower West Terrace Capitol building entrance is located. As shown in YouTube Video 2, SILLS and others attempted to follow up the stairwell where the officers had retreated but, at least at first, could not get past the locked doorway.

65. By 2:40 p.m. on January 6, 2021, rioters had engulfed the west side of the United States Capitol and were climbing on the scaffolding in front of building as well as various features of the building. Although the Capitol Building had already been breached and rioters had flooded in through several entrances, a group of MPD officers and members of the USCP or other agencies had been able to hold their position and deny entry through the very prominent entrance of the Lower West Terrace. To enter the United States Capitol through the Lower West Terrace, one must walk through a short tunnel with a series of glass doorways. Around 2:40 p.m., a group of officers were maintaining a line at the second set of glass doors inside the tunnel. Officers reporting to the scene rushed to the tunnel from within the building while rioters outside of the tunnel continued to summon more men to push their way through the tunnel. A growing number of rioters made their way into the tunnel with a variety of tools and weapons. The tunnel became the point of an intense and prolonged clash between rioters and law enforcement at the United States Capitol. Many of the rioters in the tunnel were recording video and many of the videos circulated and continue to circulate on Internet channels, social media, and the news.

66. USCP surveillance footage captures SILLS in the first group of rioters entering the tunnel. USCP surveillance shows SILLS repeatedly striking at the officers guarding the Lower West Terrace doors to the Capitol with a baton and using a strobing light to apparently try to disorient the officers.

67. Specifically, the following screenshot (with a red circle around SILLS) shows SILLS entering the mouth of the tunnel at approximately 2:41 p.m. with other rioters in the mob; he is facing the direction of the police line, which is immediately in front of the doors to the Capitol building and holds a phone in his hand.

*Screenshot from USCP Surveillance Footage at approximately 2:41 PM*



68. The same activity is captured in the Instagram Video Posted by @geoff\_sills. In that video, which as described above is a series of clips apparently filmed at the Capitol on January 6, 2021, rioters are seen approaching the tunnel where the doors are closed. An unknown rioter can be heard screaming “let us in” while another unknown rioter yells “fuck them up.” The position of the camera and the events captured corresponds to the USCP footage mentioned above showing SILL with a phone in his hand as if he were recording.

*Screenshot from the Instagram Video Posted by @geoff\_sills*



69. USCP surveillance footage then captures SILLS cheering as another rioter thrusts a flag pole in the direction of the doors, as shown in the still below with a red circle around SILLS.



*Screenshot from USCP Surveillance Footage*



70. SILLIS can then be seen grabbing his phone again and holding it up as if it is recording while the crowd moves forward. The same activity is then captured in the Instagram Video Posted by @geoff\_sills. As shown in the stills below, in the video, glass in one of the doors is now broken and the rioters can be seen opening the first set of doors and walking toward the line of officers standing shoulder to shoulder at the second set of doors. The rioters can be seen rushing forward towards the officers holding riot shields and one rioter can be seen repeatedly hitting at the officers with a pole. One rioter then yells “don’t hurt the police” while others begin chanting “U.S.A.”

*Screenshot from the Instagram Video Posted by @geoff\_sills*





71. As evidenced by the USCP surveillance footage of the tunnel (with a red circle around SILLS in the screenshot below), SILLS continued to make his way to the front of the police line while holding his phone up as if he was recording.

*Screenshot from USCP Surveillance Footage at approximately 2:43 PM*



72. At approximately 2:44 p.m., as captured on BWC from Officer 4, SILLS is with the other rioters pushing up against the officers guarding the doors. SILLS can then be seen holding up a baton in his hand (circled in red in the still below). SILLS can then be seen on Officer 4's BWC turning around and walking back out the tunnel.

*Screenshot from BWC of MPD Officer 4*



73. At approximately 2:46 p.m., SILLS exits the tunnel holding what appears to be an extended baton. As SILLS exits the tunnel into the sea of rioters, SILLS lifts the baton above his head in what appears to be an effort to signal and galvanize the crowd.

*Screenshots from USCP Surveillance Footage*



74. At approximately 2:52 p.m., SILLS raises the baton in his right hand and what appears to be a flashlight in his left hand pointed at the officers. SILLS uses the strobe and flashing function of the flashlight which, based on my training and experience, appears to have been used in order to disorient and obscure the vision of the officers.

75. For several minutes, as shown on USCP surveillance footage, using the baton, SILLS proceeds to strike the officers at and near the front of the police line numerous times with what appears to be a significant amount of force. Many of these same events described below are also captured on a video filmed by a photojournalist and posted to YouTube (hereinafter “YouTube Video 3”). They are also captured in another video uploaded to YouTube (hereinafter “YouTube Video 4”). YouTube Video 4 was filmed by another rioter (who has since been arrested) and was obtained through a search warrant of his related account.

*Screenshots from USCP Surveillance Footage*







76. At approximately 2:52p.m., SILLIS was captured on the BWC of MPD Officer 5 using the baton to strike Officer 5's left arm, as shown in the stills below with a red circle around SILLIS and/or the baton.

*Screenshots from BWC of Officer 5*





77. At approximately 2:53 p.m., using the baton, SILLS strikes at and near the officers at the front of the police line and simultaneously continues to use the flashing light against officers to hinder their vision, while another rioter to the right of SILLS uses a chemical spray against the officers, as illustrated in the screenshots below.

*Screenshots from USCP Surveillance Footage*



78. Between approximately 2:52p.m. and 3:00p.m., USCP surveillance footage captured SILLS repeatedly using the baton to strike the officers at and near the front of the police



line numerous times. At various times, SILLS gets pushed towards the back of the crowd and repeatedly makes his way forward towards the front of the police line.

*Screenshots from USCP Surveillance Footage*





79. At approximately 2:59 p.m., SILLS has the baton raised in his right hand and appears to use his left hand to signal to the other rioters to move aside so that SILLS can successfully strike the officers as opposed to accidentally striking the rioters.

*Screenshots from USCP Surveillance Footage*





80. The same is captured in YouTube Video 3 from a different angle. In YouTube Video 3, after signaling the other rioters to move over, SILLS can be seen changing his grip on the baton so that he can strike downward with it instead of swinging it. He can then be seen repeatedly striking downward with the baton at the officer in front who has his hand up, as shown in the still below with a red circle around SILLS and the officer's hand.



*Screenshot from YouTube Video 3*



81. As captured on USCP footage, at approximately 3:00 p.m., SILLS turns around and leaves the tunnel. SILLS can then be seen walking out into the crowd and lifting the baton over his head in YouTube Video 1, as shown in the stills below.

*Screenshot from YouTube Video 1*



*Connection to Electronic Evidence and Subject Device*

82. Witness 4 provided geoffsills.cgi@gmail.com and the SUBJECT PHONE NUMBER as accounts belonging to SILLS. Subscriber records obtained in response to a subpoena show SILLS is the listed account holder for geoffsills.cgi@gmail.com and the SUBJECT PHONE NUMBER is listed as the recovery phone number for the account. Subscriber records obtained in response to a subpoena for geoff.scad@gmail.com list “Geoff” with no last name provided as the account holder. However, the same SUBJECT PHONE NUMBER is listed as the recovery number, and geoff.scad@gmail.com is also listed as the recovery email for geoffsills.cgi@gmail.com. Subscriber records further show both accounts as active, with multiple IP logins between November 2020 and May 2021, including logins on January 6, 2021 and the surrounding days for geoff.scad@gmail.com.

83. Subscriber records further show that the following services were associated with geoff.scad@gmail.com: Gmail, Google Hangouts, iGoogle, Google Drive, Google Docs, YouTube, Google Calendar, Web & App Activity, Google Chrome Sync, Google Photos, Google Maps Engine, Google My Maps, Google Payments, Google Maps, Android, Dynamite.

84. Subscriber records show that the following services were associated with geoffsills.cgi@gmail.com: Web & App Activity, Gmail, Google Hangouts, Google Calendar, YouTube, Google My Maps, Google Voice, Android, Google Docs, Google Payments, Google Keep, Dynamite.

85. Similarly, subscriber records from Uber obtained in response to a subpoena also show an account for SILLS, with the same SUBJECT PHONE NUMBER listed and the geoffsills.cgi@gmail.com address.



86. In addition, your affiant has reviewed subscriber records from a Zello account linked to SILLS. Zello is a “push-to-talk” walkie-talkie application used by multiple rioters on January 6, 2021 to communicate. Subscriber records show that an account named “trump162021” is linked to both the SUBJECT PHONE NUMBER and one of the emails associated with SILLS (geoffsills.cgi@gmail.com). Records further show that the account was created on January 6, 2021 and used repeatedly on January 6, 2021.

87. A review of records provided by Verizon Wireless in response to a subpoena indicate that the mother of SILLS is currently the financially liable party for the SUBJECT PHONE NUMBER and has been a customer since March 2008. The SUBJECT PHONE NUMBER is linked to an iPhone 7 Plus with IMEI 35947508484620. Subscriber records also show that this phone was active repeatedly from January 5 to January 7, 2021, with calls made or received each day.

88. According to records obtained through a search warrant served on Verizon Wireless, the cellphone associated with the SUBJECT PHONE NUMBER was identified as having utilized a cell site consistent with providing service to a geographic area that includes the interior of the United States Capitol building on and around the date of January 6, 2021.

89. A review of records provided by Apple in response to a subpoena indicate that SILLS had an iCloud account registered to the same iPhone 7 plus, and that SILLS subscribed to iCloud Drive services.

90. As noted above, SILLS can be seen recording events on January 6, 2021 on a phone; SILLS later posted some of those recordings on his Instagram account. The phone visible in SILLS’s hand is consistent in shape and size as an iPhone.

### **SILLS's PERSON**

91. A warrant to search the person of **SILLS** is requested because **SILLS** may be found wearing or carrying clothing, eyewear, or other evidence related to the charged offenses listed herein. **SILLS** may also be carrying on his person electronic devices, including one or more mobile phones, which are also the subject of the requested search warrant.

### **The SUBJECT RESIDENCE**

92. Open source database queries provided 8276 Shane Edmonds Ln. Mechanicsville, VA 23111 as a possible address for **SILLS**. In addition, financial records obtained by subpoena further list this as the address where **SILLS** received financial statements from at least November 2020 through April 2021 (the return date of the subpoena to the financial institution). The financial records further show repeated transactions in Mechanicsville, VA that must be completed in person (such as ATM withdrawals) over the last few months.

93. On June 04, 2021, early in the afternoon, law enforcement observed a white Ford Fusion, Alabama Registration 47VL552, parked in front of 8276 Shane Edmonds Lane. This vehicle is registered to **SILLS**, who had a prior residence in Alabama. On June 14, 2021, around 2:00 PM, law enforcement again observed the listed white Ford Fusion in front of 8276 Shane Edmonds Lane. The vehicle was parked, with the driver's side tires resting in the roadway and the passenger side tires resting in the front yard of the residence.

94. On June 14, 2021, around 4:00 PM, a law enforcement agent drove by the residence and observed the listed Ford Fusion parked in the same position in front of the listed address. After the law enforcement agent turned around on an adjacent street in the same neighborhood in attempt to pass by the residence again, the law enforcement agent observed that

the listed vehicle was no longer parked in front of the residence. As the law enforcement agent exited the neighborhood, he observed the listed vehicle at the stop sign attempting to turn right onto Lee Davis Road. The law enforcement agent followed the vehicle to the intersection of Lee Davis Road and Pole Green Road, and observed the vehicle enter the Exxon Gas Station. The law enforcement agent then observed the driver exit the vehicle. The law enforcement agent believed the driver to be **SILLS**. The law enforcement agent observed **SILLS** return to the vehicle. The vehicle exited the parking lot and turned onto Pole Green Road.

95. On June 15, 2021, around 9:15 PM, law enforcement observed the listed white Ford Fusion again parked in front of 8276 Shane Edmonds Lane in the same fashion (driver's side tires resting in the roadway; passenger side tires resting in the front yard).

96. I know, based on my training and experience, that people who spend time at a particular address also store their belongings and devices as part of their daily lives at that address. Relatedly, people routinely re-wear clothing and accessories and store these items in their homes. Clothing and accessories consistent with those worn by **SILLS** (such as the black "Make America Great Again" (MAGA) hat, the distinctive striped shirt, black binoculars, a black gas mask, black and white sneakers, a white gauge ear piercing, and a black and grey backpack) constitute evidence of the commission of the offenses discussed herein, in that **SILLS** can be visually identified as the individuals in the photographs and videos discussed above, in part through the distinct attire and accessories **SILLS** wore that day. Similarly, items such as binoculars, gas masks, batons, and lights can similarly be expensive, and I know, based on my training and experience, that people who equip themselves for military-style confrontations keep such equipment for long periods of time in safe places for use in the future. Accordingly, your

Affiant submits there is probable cause to believe that a search of the **SUBJECT RESIDENCE** will reveal additional evidence of the subject offenses.

97. Moreover, because **SILLS** traveled to Washington, D.C. from Virginia, there is also probable cause to believe that **SILLS** would have obtained receipts from his travels, such as Metro receipts or a Metro card. Accordingly, your Affiant submits there is probable cause to believe that a search of the **SUBJECT RESIDENCE** will reveal additional evidence of the Subjects' motive, planning, coordination, intent, and travel to Washington, D.C.

### **SUBJECT DEVICES**

98. As referenced above, **SILLS** can be seen recording the events of January 6, 2021 on video and BWC footage. Specifically, **SILLS** can be seen holding a device similar in shape and size to an iPhone, and videos corresponding to those events were subsequently posted to **SILLS**'s Instagram account (with captions presumably added by **SILLS**).

99. In addition, based on photos and videos of the offenses that date, numerous persons committing the Target Offenses possessed digital devices that they used to record and post photos and videos of themselves and others committing those offenses. Further, based on the investigation, numerous persons committing the Target Offenses possessed digital devices to communicate with other individuals to plan their attendance at the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings. Moreover, it is well-known that virtually all adults in the United States use mobile digital devices. In a fact sheet from June 12, 2019, The Pew Research Center for Internet & Technology estimated that 96% of Americans owned at least one cellular phone, and that that same 2019 report estimated that 81% of Americans use at least

one smartphone. *See* Mobile Fact Sheet, <https://www.pewresearch.org/internet/fact-sheet/mobile/> (last visited Jan. 9, 2021).

100. In addition, in my training and experience, it is common for individuals to back up or preserve copies of digital media (such as photos and videos) across multiple devices to prevent loss. Indeed, some companies provide services that seamlessly sync data across devices, such as Apple devices and the Apple iCloud service. Thus, there is reason to believe that evidence of the offenses that originally resided on SILLS's cell phone may also be saved to other digital devices within the SUBJECT RESIDENCE or on SILLS's person. Moreover, here, as widely reported in the news media related to this matter, many individuals committing the Target Offenses kept and posted videos, photos, and commentary about their participation in these offenses, essentially bragging about their participation. Based on that, there is also probable cause to believe that evidence related to these offenses may have been transferred to and stored on digital devices beyond the particular digital device SILLS possessed during the offenses.

101. In addition, as described above, there is evidence that there was repeated activity (such as calls and logins) with electronic accounts associated with SILLS, and initial cell evidence for the Subject Number is consistent with providing service to a geographic area that includes the interior of the United States Capitol building on and around the date of January 6, 2021. For instance, SILLS's Zello account (which is a push to talk service for phones used by multiple rioters on January 6, 2021) shows multiple logins on January 6, 2021. As a result, there is reason to believe that SILLS had the Subject Phone with him on January 6, 2021, and that evidence relating to the offenses will be found on the Subject Phone.



102. Based on my training and experience, I know that crimes carried out by more than one person often involve some amount of communication among those involved. This may involve working out details of and preparing to carry out a premeditated crime, working together to cover up the crime afterwards, or simply arranging to meet up someplace where an unplanned crime would later occur. Either way, I know from training and experience that phones are often used for this purpose and that phones used by a participant in such criminal activity often contains evidence of communication among accomplices. For instance, communication logs indicate who the account user was communicating with both immediately before and after the crime. Similarly, your affiant has seen multiple examples of suspects communicating after a crime via text (or other online chat functions like Google Hangouts or Telegram) to discuss where incriminating items have been hidden, where and what the police are doing to investigate the crime, and whether any witnesses have implicated them. This case involves many different people, including SILLS, working together to breach the Capitol and attack the officers defending the Capitol on January 6, 2020. For instance, thus far multiple individuals have been identified as having participated in the attacks on the officers by the Lower West Terrace door of the Capitol. By its very nature, such concerted action amongst multiple people in varying locations involves discussion and planning, which is regularly done by online chats or texts. Indeed, law enforcement has already identified multiple texts, chats, and social media postings in other cases regarding plans for activity at the Capitol on January 6, 2021 and discussions of the events after the fact. Such discussions and posts often lead to discussions online about the account user's specific plans and state of mind regarding the events on January 6, 2021, as well as evidence of co-conspirators. In this case, there is evidence that SILLS used his online accounts to display his activities on January 6, 2021 (such as videos SILLS posted of the riot). He also made multiple

calls and texts on January 6, 2021, including via an online communication platform (Zello) that SILLS downloaded that day. Although SILLS appears to have deleted the social media account he used to post video of the riot, social media accounts are often linked to Google accounts, which are often backed up to a user's phone, will have relevant evidence in this case, as users typically receive emails from social media providers about their online accounts. Similarly, as users typically post content initially recorded on their phones, even videos deleted from social media will often still be found on the user's phone. In addition, to the extent SILLS reserved a room or arranged for travel to Washington D.C., something which is often done via email, it is likely that evidence of SILLS's involvement in the crime will be found on SILLS's online accounts, and backed up to the Subject Phone, as there is likely to be related email exchanges for such types of reservations.

103. Based on my training and experience, I know that victims, witnesses, and perpetrators of crimes often communicate between and among themselves before, during, and after the crime. They communicate using text messaging, apps, social media, and calls via both typical phone calls and App-enabled calling methods. In my training and experience, communications between suspects have revealed the identities and relationships between and among the involved individuals, as well as their motive, hostility, knowledge, and intent relating to the crime. Moreover, such communications have also revealed consciousness of guilt and efforts to impede police investigation, such as threats sent to witnesses or victims after a crime. Similarly, they are often featured in photographs and/or video recordings together, which provide key evidence in demonstrating the nature of their relationship. In addition, an examination of a contact list is often critical in establishing these relationships, as people who know each other typically have each other's information in their contact lists, and people are unlikely to have

complete strangers included in such lists. For example, your affiant has already identified such evidence on the social media postings by SILLS, specifically the Instagram video posted documenting the day. Additional evidence of such communications is also likely given that SILLS appears to have signed up for a Zello account (something used by multiple rioters to communicate on January 6, 2021), and that account is tied to one of SILLS's Google email accounts. As such, evidence of the SILLS's intent and state of mind is likely to be found in discussions between the SILLS and his unidentified co-conspirators, along with evidence about the identity of such co-conspirators.

104. Based on my training and experience, I know that witnesses, and even perpetrators, often record criminal activity. For example, witnesses have recorded school fights, attacks on public transportation, and police shootings and assaults. Law enforcement has seen such videos shared and discussed amongst co-conspirators or friends through online accounts. These videos have proven extremely crucial in investigations by depicting the crime itself. Similarly, law enforcement has seen criminals take photographs of their victims and of themselves with the proceeds of a crime shortly after committing it. In this case in particular, your affiant has already identified some video recordings of SILLS's involvement in the storming of the Capitol on January 6, 2021, as described above. Your affiant believes that it is likely that additional photographs or videos of this nature will be found on the SUBJECT PHONE.

105. In addition, your affiant also knows through training and experience that, just like most people, criminals often keep photos and videos of themselves on their phones. These photos and videos capture the clothes they own and wear at the time of the photograph, which is relevant in identifying the individual in videos and photographs from the breach of the Capitol. In this case, in addition to videos or photographs of January 6, 2021, photographs of

SILLS with the striped shirt, backpack, gauged earrings, gas mask, or other clothing he can be seen wearing in the surveillance video described above will be key evidence in the case. Indeed, your affiant has already identified examples of photographs of SILLS in the same shirt SILLS wore on January 6, 2021.

106. Based on my training and experience, I know that people who commit crimes often use their cell phones to capture and store images or video recordings of related contraband – sometimes called “trophy photos” – such as photos of any items taken during the breach of the Capitol. They also often share these images or video recordings with associates using text messaging or other forms of communication on their cell phone. This is particularly common on social media sights like Instagram or Facebook, where users can share videos and photos with a limited online audience. Such videos, photos, and chats about the videos and photos are then often stored in their related phones. Your affiant believes that it is likely additional photographs or videos of this nature will be found on the Subject Phone – particularly considering that SILLS can be seen recording the events on January 6, 2021.

107. Based on my training and experience, I know that people who purchase specialized equipment, like the binoculars, baton, gas masks, binoculars, or flashing light used by SILLS on January 6, 2021, often receive emails related to their purchases. In this case, there is evidence that SILLS made multiple purchases in November 2020 from shops that sell such tactical equipment. Because many of these stores were online, it is likely that the purchases involved email communications, such as emails with the receipt or confirmation of the purchase. Because such email communications are then recoverable through the user’s phone, there is reason to believe that evidence of this nature is likely to be found on the Subject Phone.

108. Based on my training and experience, I know that individuals involved in criminal activity often use their cell phones to search the internet to learn the status of a criminal investigation, i.e., look up the newspaper articles about the crime, determine if the police have suspects, and learn the identity of witnesses. For example, law enforcement has regularly seen suspects look up articles chronicling developments in the case, reward posters, news about the particular location the crime occurred, news about the type of crime committed, YouTube videos posted by police, and news from FBI's informational sites. Similarly, based on my training and experience, I know that individuals involved in criminal activity often use their cell phones to search the internet in preparation for a crime, such as researching new weapons or looking up information on victims or witnesses. This case in particular has been heavily covered by the media, with video footage of rioters (including of SILLIS) appearing on national news. Your affiant has repeatedly seen other rioters conduct searches about developments in the case or related searches indicating they participated in the riots. As a result, in this case, there is reason to believe that the account's internet search history is likely to contain evidence of the suspect's involvement in the crime and state of mind regarding the crime.

109. Based on my training and experience, I know that people who commit crimes often use their phones and online accounts in ways that reveal their location and/or activities before, after, or while engaging in criminal activity. For example, this may include location information (e.g., GPS data or IP login information) and images or video recordings relevant to the criminal activity. For example, online accounts such as Google log the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the



crime under investigation. Such information allows investigators to understand the geographic and chronological context of account access, use, and events relating to the crime under investigation. Additionally, law enforcement has repeatedly seen videos or photos on a suspect's phone or social media account taken at or near key points in the crime. Such video and image files often include identifying landmarks, buildings, or backgrounds that help place the suspect at an important location related to the crime or have even exculpated the individual by placing the individual at a different location at the time of the crime. Such videos or selfies that were taken at or near the time of the crime inculcate or exculpate the suspect by identifying the phone user's precise location at the time the photo or video was taken. Furthermore, I know from training and experience messages sent via texts or on an apps often include communications that shed light on the user's location and activity during a particular time period. For example, just as people making plans often update each other via text regarding when they will arrive somewhere or where they will meet, suspects often message with co-conspirators, friends, or other confidants on social media regarding where they are going or when they plan on arriving to a location. Indeed, in this case, SILLS posted about the events on his social media account updating others about SILLS's participation in the events in Washington D.C. on January 6, 2021. As such it seems likely that SILLS made similar comments on his related online accounts. Similarly, given the initial cell site data linking SILLS to the Capitol on January 6, 2021, evidence of SILLS's use of the related SUBJECT NUMBER on that day is in itself evidence of his location. Specifically, calls, texts, and other information on the SUBJECT PHONE showing that SILLS used that Subject Number before and after the event will provide evidence in the case of SILLS's involvement (or lack thereof) in the riots on January 6, 2021.

110. Based on my training and experience, I know that suspects often delete incriminating items (such as photos, videos, texts, internet searches, and other communications) after committing a crime or learning that law enforcement have developed leads. This evidence is often highly relevant evidence, as it tends to be particularly incriminating. For example, your affiant is aware of suspects deleting incriminating searches for news about the crime, texts or messages with coconspirators planning crimes, and texts or messages confessing to the crime. The very fact that the items are deleted make them much more likely to be probative in the investigation. Deleted items, such as a deleted search about the specific weapon used in the crime, a deleted search regarding news about a crime at that particular location, or a deleted text discussing details of the crime, are often still probative even without a date as they often provide direct and substantial evidence of the suspect's state of mind and involvement in the crime. Here, there is already evidence of SILLS taking steps to delete data associating him with the crime, as SILLS's Instagram account was deleted after the postings described above. As a result, in this case there is reason to believe that deleted items in the Subject Phone are likely to contain evidence of the SILLS's involvement in the riots.

111. Based on my training and experience, I know that phones typically list device information (such as the associated IMEI, Phone Number, Android or Apple ID) and linked user accounts. The device information, includes for instance the phone numbers associated with the phone, the IMEI, and sometimes even includes the name of the phone as provided by the phone user (such as "JohnDoe's I-phone"). Linked user accounts include account names and handles used to log in to Apps regularly used on the phone, such as the account names used on social media sites like Instagram, email accounts used, or online communication platforms, like Textnow and Snapchat. Both device information and linked accounts are key both for identifying

the phone user's location during the crime and for identifying the user of the phone. Device information and linked accounts are typically then the basis of key additional investigative steps that allow law enforcement to identify the phone user's location at the time of the crime. For example, once the active phone number used by the suspect is identified, law enforcement can then apply for a cell site warrant, which provides location data on the phone user. Similarly, once an email account or Apple ID is identified, law enforcement may be able to apply for a warrant for location data stored by that online provider, such as Google location records. Based on my training and experience, I know that linked accounts, such as a cell phone number or a related email account, also provide key information to indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, if the phone number associated with the phone is a number frequently used by friends or associates of the suspect to contact him or her, the government's identification of the phone number will assist in proving who was using the phone at the time key activity on the phone occurred. Similarly, your affiant has regularly seen the suspect's full name be listed in the email address linked to a phone, which clearly helps identify the user of the phone. As such, in this case the phone number, email addresses, and related user profiles on social media platforms or communication applications are evidence that will likely yield additional investigative leads as to SILLS's location in the relevant times surrounding the crimes, and provide evidence of who was using the Subject Phone at the time of the crimes.

112. Based on my training and experience, the term "wireless telephone," also known as a mobile telephone, cellular telephone, or smartphone, means a handheld wireless device used for voice and data communication through radio signals. These telephones send

signals through networks of transmitters/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device. Other mobile and home computing devices feature similar technologies and capabilities.

113. Your Affiant submits that there is probable cause to believe that there exists physical and/or electronic evidence related to the commission of the offenses listed above on the mobile telephones used by SILLS, including photographic, video, and other electronic evidence indicative of SILL’S movements, location, motivation, planning, and communications related to the offenses listed herein, and the identities of co-conspirators and other individuals violating federal law during their entry into the U.S. Capitol, among other things.

**DIGITAL DEVICES, ELECTRONIC/MAGNETIC STORAGE, AND**  
**FORENSIC ANALYSIS**

114. As described above and in Attachment B, this application seeks permission to search for evidence, instrumentalities, and information that might be found within the **SUBJECT DEVICES**, in whatever form they are found. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the

forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the **SUBJECT DEVICES** for at least the following reasons:

a. Individuals who engage in the foregoing criminal activity, in the event that they change digital devices, will often “back up” or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

b. Digital device files, or remnants of such files, can be recovered months or even many years after they have been downloaded onto the medium or device, deleted, or viewed via the Internet. Electronic files downloaded to a digital device can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensics tools. When a person “deletes” a file on a digital device such as a home computer, a smart phone, or a memory card, the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the digital device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are



replaced with more recently viewed Internet pages. Thus, the ability to retrieve “residue” of an electronic file from a digital device depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer, smart phone, or other digital device habits.

115. As further described in Attachment B, this application seeks permission to locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this affidavit, but also for forensic electronic evidence or information that establishes how the **SUBJECT DEVICES** were used, the purpose of their use, who used them (or did not), and when. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit there is probable cause to believe that this forensic electronic evidence and information will be in the **SUBJECT DEVICES** at issue here because:

a. Although some of the records called for by this warrant might be found in the form of user-generated documents or records (such as word processing, picture, movie, or texting files), digital devices can contain other forms of electronic evidence as well. In particular, records of how a digital device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials contained on the digital device(s) are, as described further in the attachments, called for by this warrant. Those records will not always be found in digital data that is neatly segregable from the hard drive, flash drive, memory card, or other electronic storage media image as a whole. Digital data stored in the **SUBJECT DEVICES**, not currently associated with any file, can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of

a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on a hard drive that show what tasks and processes on a digital device were recently used. Web browsers, e-mail programs, and chat programs often store configuration data on a hard drive, flash drive, memory card, or memory chip that can reveal information such as online nicknames and passwords. Operating systems can record additional data, such as the attachment of peripherals, the attachment of USB flash storage devices, and the times a computer, smart phone, or other digital device was in use. Computer, smart phone, and other digital device file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, indicate the identity of the user of the digital device, or point toward the existence of evidence in other locations. Recovery of this data requires specialized tools and a controlled laboratory environment, and also can require substantial time.

b. Forensic evidence on a digital device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, chats, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the digital device at a relevant time, and potentially who did not.

c. A person with appropriate familiarity with how a digital device works can, after examining this forensic evidence in its proper context, draw conclusions about how such digital devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a digital device that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, digital device evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on digital devices is evidence may depend on other information stored on the devices and the application of knowledge about how the devices behave. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a digital device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on the device. For example, the presence or absence of counter-forensic programs, anti-virus programs (and associated data), and malware may be relevant to establishing the user's intent and the identity of the user.

#### **METHODS TO BE USED TO SEARCH DIGITAL DEVICES**

116. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I know that:

a. Searching digital devices can be an extremely technical process, often requiring specific expertise, specialized equipment, and substantial amounts of time, in part because there are so many types of digital devices and software programs in use

today. Digital devices – whether, for example, desktop computers, mobile devices, or portable storage devices – may be customized with a vast array of software applications, each generating a particular form of information or records and each often requiring unique forensic tools, techniques, and expertise. As a result, it may be necessary to consult with specially trained personnel who have specific expertise in the types of digital devices, operating systems, or software applications that are being searched, and to obtain specialized hardware and software solutions to meet the needs of a particular forensic analysis.

b. Digital data is particularly vulnerable to inadvertent or intentional modification or destruction. Searching digital devices can require the use of precise, scientific procedures that are designed to maintain the integrity of digital data and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Recovery of “residue” of electronic files from digital devices also requires specialized tools and often substantial time. As a result, a controlled environment, such as a law enforcement laboratory or similar facility, is often essential to conducting a complete and accurate analysis of data stored on digital devices.

c. Further, as discussed above, evidence of how a digital device has been used, the purposes for which it has been used, and who has used it, may be reflected in the absence of particular data on a digital device. For example, to rebut a claim that the owner of a digital device was not responsible for a particular use because the device was being controlled remotely by malicious software, it may be necessary to show that malicious software that allows someone else to control the digital device remotely is not present on the digital device. Evidence of the absence of particular data or software on a

digital device is not segregable from the digital device itself. Analysis of the digital device as a whole to demonstrate the absence of particular data or software requires specialized tools and a controlled laboratory environment, and can require substantial time.

d. Digital device users can attempt to conceal data within digital devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear as though the file contains text. Digital device users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. Digital device users may encode communications or files, including substituting innocuous terms for incriminating terms or deliberately misspelling words, thereby thwarting “keyword” search techniques and necessitating continuous modification of keyword terms. Moreover, certain file formats, like portable document format (“PDF”), do not lend themselves to keyword searches. Some applications for computers, smart phones, and other digital devices, do not store data as searchable text; rather, the data is saved in a proprietary non-text format. Documents printed by a computer, even if the document was never saved to the hard drive, are recoverable by forensic examiners but not discoverable by keyword searches because the printed document is stored by the computer as a graphic image and not as text. In addition, digital device users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography, a digital device user can conceal text in an image file that cannot be viewed when the image file is opened. Digital devices may also contain “booby traps”



that destroy or alter data if certain procedures are not scrupulously followed. A substantial amount of time is necessary to extract and sort through data that is concealed, encrypted, or subject to booby traps, to determine whether it is evidence, contraband, or instrumentalities of a crime.

e. Analyzing the contents of mobile devices can be very labor intensive and also requires special technical skills, equipment, and software. The large, and ever increasing, number and variety of available mobile device applications generate unique forms of data, in different formats, and user information, all of which present formidable and sometimes novel forensic challenges to investigators that cannot be anticipated before examination of the device. Additionally, most smart phones and other mobile devices require passwords for access. For example, even older iPhone 4 models, running IOS 7, deployed a type of sophisticated encryption known as “AES-256 encryption” to secure and encrypt the operating system and application data, which could only be bypassed with a numeric passcode. Newer cell phones employ equally sophisticated encryption along with alpha-numeric passcodes, rendering most smart phones inaccessible without highly sophisticated forensic tools and techniques, or assistance from the phone manufacturer. Mobile devices used by individuals engaged in criminal activity are often further protected and encrypted by one or more third party applications, of which there are many. For example, one such mobile application, “Hide It Pro,” disguises itself as an audio application, allows users to hide pictures and documents, and offers the same sophisticated AES-256 encryption for all data stored within the database in the mobile device.

f. Based on all of the foregoing, I respectfully submit that searching any digital device for the information, records, or evidence pursuant to this warrant may require a wide array of electronic data analysis techniques and may take weeks or months to complete. Any pre-defined search protocol would only inevitably result in over- or under-inclusive searches, and misdirected time and effort, as forensic examiners encounter technological and user-created challenges, content, and software applications that cannot be anticipated in advance of the forensic examination of the devices. In light of these difficulties, your Affiant requests permission to use whatever data analysis techniques reasonably appear to be necessary to locate and retrieve digital information, records, or evidence within the scope of this warrant.

117. In searching for information, records, or evidence, further described in Attachment B, law enforcement personnel executing this search warrant will employ the following procedures:

a. The digital devices, and/or any digital images thereof created by law enforcement, sometimes with the aid of a technical expert, in an appropriate setting, in aid of the examination and review, will be examined and reviewed in order to extract and seize the information, records, or evidence described in Attachment B.

b. The analysis of the contents of the digital devices may entail any or all of various forensic techniques as circumstances warrant. Such techniques may include, but shall not be limited to, surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); conducting a file-by-file review by “opening,” reviewing, or reading the images or first few “pages” of such files in order

to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “keyword” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

c. In searching the digital devices, the forensic examiners may examine as much of the contents of the digital devices as deemed necessary to make a determination as to whether the contents fall within the items to be seized as set forth in Attachment B. In addition, the forensic examiners may search for and attempt to recover “deleted,” “hidden,” or encrypted data to determine whether the contents fall within the items to be seized as described in Attachment B. Any search techniques or protocols used in searching the contents of the **SUBJECT DEVICES** will be specifically chosen to identify the specific items to be seized under this warrant.

**BIOMETRIC UNLOCK OF DEVICES SUBJECT TO WARRANT**

118. I ask that the search warrant, to the extent it authorizes the seizure and search of electronic devices, also authorize the use of the biometric unlock features on any such devices, based on the following, which I know from my training, experience, and review of publicly available materials.

119. The make and model of the current **SUBJECT DEVICES** are unknown to this Affiant. Although SILLS is associated with an iPhone 7 at the time of the crimes in question, it is possible SILLS may have upgraded or changed phones since then. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption

systems protect the contents of these devices from unauthorized access by users and render these contents unreadable to anyone who does not have the device's password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

120. I also know that many digital devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

121. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

122. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on

an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

123. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress **SILLS'S** thumb-and/or fingers on the device(s); and (2) hold the device(s) in front of **SILLS'S** face with his eyes open to activate the facial-, iris-, and/or retina-recognition feature.



**V. Conclusion**

124. Based on the facts set forth above, your Affiant respectfully submits that there is probable cause to believe that **SILLS** and others engaged in violations of the Target Offenses. Furthermore, there is probable cause that evidence and instrumentalities of these violations (described with more specificity in Attachment B to this affidavit) are presently located on **SILLS'S PERSON**, at the **SUBJECT RESIDENCE**, and on the **SUBJECT DEVICES** as described in Attachment A to this affidavit.

125. Accordingly, your Affiant respectfully requests that the Court issue a search warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure authorizing FBI agents and representatives of the FBI, with assistance from representatives of other law enforcement agencies as required, to search **the person of SILLS, the residence located at 8276 Shane Edmonds Lane, Mechanicsville, VA 23111, and mobile devices belonging to SILLS** (more precisely described in Attachment A), for evidence and instrumentalities (more precisely described in Attachment B).



Benjamin Fulp  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on June 17, 2021

/s/ 

Mark R. Colombell  
United States Magistrate Judge

**ATTACHMENT A**

**ITEMS/PERSONS/LOCATIONS TO BE SEARCHED**

1. **SILLS's PERSON:** The person to be searched is the person of **Geoffrey William Sills**, including any clothing, mobile telephones, digital devices, personal effects, backpacks, wallets, briefcases, and bags that are on **SILLS's** person or within **SILLS's** immediate vicinity and control at the location where the search warrant is executed. Photographs depicting **SILLS**, a Caucasian male who resides in Mechanicsville, Virginia, with date of birth 4/17/1991, are shown below.



2. **The SUBJECT RESIDENCE:** The premises to be searched are located at **8276 Shane Edmonds Lane, Mechanicsville, VA 23111**, which is further described as a two story white single family home, with dark shutters, a light green front door, and a light green door on the side near the driveway. The **SUBJECT RESIDENCE** is depicted in the following images:



3. **SUBJECT DEVICES:** The devices to be searched are mobile phones in the possession of **SILLS** or mobile devices located at the **SUBJECT RESIDENCE** available for use by **SILLS**.

---

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

1. The items to be seized are evidence, information, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 1512(c)(2) (obstruction of Congress); 111 (assaulting a federal agent); 231 (civil disorders); 371 (conspiracy); 372 (conspiracy to impede or injure officer); 930 (possession of firearms and dangerous weapons in federal facilities); 641 (theft of government property); 1361 (destruction of government property); 2101 (interstate travel to participate in riot); 1752(a)(1), (2) and (4) (unlawful entry on restricted buildings or grounds); and Title 40 U.S.C. Section 5104(e)(2) (violent entry, disorderly conduct, and other offenses on capitol grounds) (the “Target Offenses”) that have been committed by **Geoffrey William Sills** (“the Subject” or “SILLS”), and other identified and unidentified persons, as described in the search warrant affidavit; including, but not limited to:

- a. Evidence concerning planning to unlawfully enter the U.S. Capitol, including any maps or diagrams of the building or its internal offices;
- b. Evidence concerning unlawful entry into the U.S. Capitol, including any property of the U.S. Capitol;
- c. Evidence concerning awareness of the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
- d. Evidence concerning efforts to disrupt the official proceeding that was to take place at Congress on January 6, 2021, i.e., the certification process of the 2020 Presidential Election;
- e. Evidence concerning the breach and unlawful entry of the United States Capitol, and any conspiracy or plan to do so, on January 6, 2021;
- f. Evidence concerning the riot and/or civil disorder at the United States Capitol on January 6, 2021;



- g. Evidence concerning the assaults of federal officers/agents and efforts to impede such federal officers/agents in the performance of their duties the United States Capitol on January 6, 2021;
  - h. Evidence of any conspiracy, planning, or preparation to commit those offenses;
  - i. Evidence concerning efforts after the fact to conceal evidence of those offenses, or to flee prosecution for the same;
  - j. Evidence concerning materials, devices, or tools that were used to unlawfully enter the U.S. Capitol by deceit or by force, including weapons and elements used to breach the building or to counter efforts by law-enforcement, such as pepper spray or smoke grenades;
  - k. Evidence of communication devices, including closed circuit radios or walkie-talkies, that could have been used by co-conspirators to communicate during the unlawful entry into the U.S. Capitol;
  - l. Evidence of the state of mind of the subject and/or other co-conspirators, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation; and
  - m. Evidence concerning the identity of persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the unlawful actors about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts.
2. Records and information that constitute evidence of identity, including but not

limited to:

- a. clothing worn by **SILLS**, to include a black “Make America Great Again” (MAGA) hat, a distinctive striped shirt, black binoculars, a black gas mask, black and white sneakers, a white gauge ear piercing, and a black and grey backpack;
- b. clothing and other articles that reflect evidence of having participated in the unlawful activity at the U.S. Capitol, including evidence of pepper spray or other non-lethal crowd control remnants;
- d. Other paraphernalia used by or associated with the Subjects, to include a black binoculars, gas mask, baton, or flashlight.

3. Records and information—including but not limited to documents, communications, emails, online postings, photographs, videos, calendars, itineraries, receipts, and financial statements—relating to:

- a. Any records and/or evidence revealing the Subject's presence at the January 6, 2021, riot;
- b. Any physical records, such as receipts for travel, which may serve to prove evidence of travel of to or from Washington D.C. from December of 2020 through January of 2021;
- c. The Subject's (and others') motive and intent for traveling to the U.S. Capitol on or about January 6, 2021;
- d. The Subject's (and others') activities in and around Washington, D.C., specifically the U.S. Capitol, on or about January 6, 2021;

4. The **SUBJECT DEVICES**, as described in the Affidavit and Attachment A. For the **SUBJECT DEVICES**:

- a. evidence of who used, owned, or controlled the **SUBJECT DEVICES** at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;
- b. evidence of software, or the lack thereof, that would allow others to control the **SUBJECT DEVICES**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the attachment to the **SUBJECT DEVICES** of other storage devices or similar containers for electronic evidence;
- d. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICES**;
- e. evidence of the times the **SUBJECT DEVICES** was used;
- f. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT DEVICES**;

- g. documentation and manuals that may be necessary to access the **SUBJECT DEVICES** or to conduct a forensic examination of the **SUBJECT DEVICES**;
- h. records of or information about Internet Protocol addresses used by the **SUBJECT DEVICES**;
- i. records of or information about the **SUBJECT DEVICES**' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

During the execution of the search of the **SUBJECT PREMISES** and **SILLS**, as described in Attachment A, law enforcement personnel are also specifically authorized to obtain from **SILLS** (but not any other individuals present at the **SUBJECT PREMISES** at the time of execution of the warrant) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint, facial characteristics, or iris display) necessary to unlock any **SUBJECT DEVICES** requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the aforementioned person(s)' physical biometric characteristics will unlock the **SUBJECT DEVICES**, to include pressing fingers or thumbs against and/or putting a face before the sensor, or any other security feature requiring biometric recognition:

- a. any of the **SUBJECT DEVICES** found at the **SUBJECT PREMISES**,
- b. where the **SUBJECT DEVICES** are limited to those which are capable of containing and reasonably could contain evidence, information, or instrumentalities of the offense(s) as described in the search warrant affidavit and warrant attachments, for the purpose of attempting to unlock the **SUBJECT DEVICES**' security features in order to search the contents as authorized by this warrant.

While attempting to unlock the **SUBJECT DEVICES** by use of the compelled display of biometric characteristics pursuant to this warrant, law enforcement is not authorized to demand that the aforementioned person(s) state or otherwise provide the password or identify the specific biometric characteristics (including the unique finger(s) or other physical features), that may be used to unlock or access the **SUBJECT DEVICES**. Nor does the warrant authorize law enforcement to use the fact that the warrant allows law enforcement to obtain the display of any biometric characteristics to compel the aforementioned person(s) to state or otherwise provide that information. However, the voluntary disclosure of such information by the aforementioned person(s) is permitted. To avoid confusion on that point, if agents in executing the warrant ask any of the aforementioned person(s) for the password to any **SUBJECT DEVICES**, or to identify which biometric characteristic (including the unique finger(s) or other physical features) unlocks any **SUBJECT DEVICES**, the agents will not state or otherwise imply that the warrant requires the person to provide such information, and will make clear that providing any such information is voluntary and that the person is free to refuse the request.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, FBI agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. This investigation is presently covert and the government believes that the subjects of the search are not aware of this warrant.

Your Affiant requests the search warrant for the aforementioned items to include the opening and searching of any locked safes, boxes, and compartments.